REMARKS

This application has been reviewed in light of the Office Action dated May 29, 2007. Claims 1-21 are pending in this application, with Claim 1, 10, 19 and 20 being in independent form. As mentioned above, none of the claims have been amended in this Response. Favorable reconsideration is respectfully requested.

The Office Action rejected claims 1-9 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that Applicant regards as the invention. Applicant respectfully traverses this rejection. Applicant submits that claim 1 is clear in that the client:

- first receives a nonce numerical value from the server in response to an authentication request (see features of claim 1 "receiving from a client computer an authentication request containing a clients username to a server" and "said server responding with an N byte nonce numerical value"), and

- then computes a hash value using a hash algorithm and parameters among which the nonce value (see feature of claim 1 "said authentication request comprising a hash value of at least the parameters clients password, client computer unique IP address, and said nonce value").

For these reasons, Applicant believes that it is clear that the client first receives a nonce value from the server and then computes a hash value of the nonce value and other parameters.

Then, the client transmits the computed hash value to the server for accessing services (see feature of claim 1 "receiving said hash value from said client computer ...").

The Office Action rejected Claim 19 under 35 U.S.C. § 101, asserting that the claim is directed to non-statutory subject matter. Applicant respectfully traverses this rejection and asserts that the medium recited in claim 19 is a physical medium and is therefore tangible; as further evidence, the medium is expressly recited to as being between two physical entities, i.e., a client computer and a server, and therefore is tangible.

The Office Action rejected claims 1-21 under 35 U.S.C. § 103(a) as being unpatentable over U.S. published Application No. 2004/0187024 (Briscoe). in view of U.S. published Application No. 2004/0249974 (Alkhatib). Applicant respectfully traverses this rejection for the reasons stated below.

Applicant submits that the present invention as defined by the claims differs from Briscoe in that the authentication procedure is a simple one-step process while at the same time being secure against man-in-the-middle attacks. The present invention as defined by the claims also differs in that the authentication method does not rely upon the existence of other clients within the network. In contrast, Briscoe teaches an authentication method that consists of two steps, namely 1) distribution of authentication information among the clients of the network (§ [0045] – [0054]), and 2) authentication of a network client using the authentication information of at least three other clients within the network (§ [0059] – [0066]).

The first step in Briscoe consists of an exchange of messages between a client and the server. As described in paragraph [0045], the client first creates a cookie which it sends to the server along with the server's IP address and the client's IP address, i.e. the client message consists of the cookie and the two IP addresses. The cookie comprises a hash of the server's IP address, the client's IP address and a local secret Ka belonging to the client.

As further described in paragraph [0046], upon receipt of the cookie the server creates a message of its own including a cookie of its own. This cookie comprises the hash of the server's IP address, the client's IP address, the current time parameter, and the server's local secret Kb. The server's message is also signed with a hash of the client's cookie, so that the client can verify the message by regenerating its own cookie from this signature hash.

When the client receives a message from the server, as described in paragraph [0051], the client compares the signature with its own cookie. If, e.g., the comparison is successful, the client acknowledges the message by returning a message that includes the server's signature, the time parameter, and a signature comprising a hash of the server's cookie. The server regenerates the client's signature cookie and compares it with its own. If this comparison is also successful, the server transmits the authentication information, in the form of a client secret (which is distinct from the client's local secret) and a secret client ID, to the client.

The second step in Briscoe consists of the authentication itself. When it is required to authenticate a client [0059],

"the server sends an authentication request message requesting from that client authentication information which is stored by other clients in the network."

Thus, in the authentication request, as described in paragraph [0061], the client is instructed to seek authentication information from (three) other clients of the network, the other clients from which the information is gathered are chosen randomly. The server's authentication request also includes, as described in paragraph [0062], a server signature comprising a hash of the secret client ID and the authentication information, i.e. client secret, stored by the client. The server also sends, as described in paragraph [0063], in its authentication request a parameter to allow it to verify the response of the client. More specifically, paragraph [0063] states "[i]n the present embodiment, the parameter sent by the server to authenticate the response of the client is a hash of the local server secret information Ka and the current time parameter t, and will be referred to as "time confidential information", TCI." Then, as described in paragraph [0064], the client's response to the authentication request is verified using two signatures, where the first is the TCI. The second signature uses the client's verification information, i.e. secret client ID, and its authentication information, i.e. client secret. If the server is able to match both signatures, the server processes the message.

Turning now to the present invention as recited in the claims, the technical effect resulting from the exchange of a nonce and a hash comprising several parameters is that a very simple procedure for authentication of clients in a network is provided, which procedure also is at the same time secure against man-in-the-middle attacks.

The simple procedure according to the present invention as defined by the claims comprises the steps that the server receives from a client computer an authentication request containing a clients username providing such services, from which request the server identifies the client's IP address and password. The server then responds by sending an N byte nonce numerical value. The authentication request includes a hash value of at least the parameters client's password, client computer's IP address, server's IP address, and the nonce value. The server receives the hash value from the client computer as an authenticator for access to the services. The server reproduces the hash value utilizing the hash algorithm and the parameters client's password, client computer's IP address, server's IP address, and the nonce value. The server compares the hash value with the one received from the client, and grants access to the server and services only upon successful comparison.

The security against man-in-the-middle attacks is high since only the hash values are being exchanged between the client computer and the server, and because the hash value is

computed using parameters which are either not being transmitted through the network in a bare form, thus not being exposed to potential intruders, or a bare parameter which is used once and only once, thus of no use for potential intrusion into the server.

In addition, the hash value is computed from a plurality of parameters, which thus enhances the security in the communication although the hash value may be observed by a potential intruder. It is a non-trivial, and in fact, extremely difficult task to calculate backwards and extract all the used parameters even though the hash algorithm may be known to the potential man-in-the-middle attacker.

The simplicity of the procedure as defined by the claims is therefore an important factor in being secure against man-in-the-middle attacks.

In regard to the prior art rejection, starting with Briscoe, it is not obvious for a person skilled in the art to achieve the solution according to the present invention as defined by the claims since Briscoe teaches a two-step solution to an authentication process based on the [0010] complex topology of typical networks, where a client gathers authentication information (that was distributed among the clients in the first step) of a collection of other clients and uses this information to acquire access to the server. The first step of the authentication procedure, as described in paragraphs [0041] – [0054], consists of the distribution of the authentication information among the clients within the network, is a complicated process which involves the exchange of several messages and signatures between the client and the server. In other words, this means that the actual authentication process, i.e. the second step, can take place only after this initial first step. The second step, in turn, is a process that utilizes the complex topology of the network, in that the information used for the authentication is distributed through different channels in the network, as described in paragraph [0010]. While the information coming from different sources follows diversified paths on the network, thus making interception of all the authentication messages difficult, a simplification of this method by making use of only one path for information exchange leads to an insecure and highly penetrable network which a person skilled in the art would likely avoid at all cost.

Moreover, the information exchanged between the server and the client in the initial step, involves several transmissions of several parameters in bare form which thus can be exposed to a potential man-in-the-middle attacker. However, thanks to the use of diversified

paths such exposure is of little significance since it would be difficult for a potential intruder to gather all the necessary information.

Starting from the teaching of Briscoe, a person skilled in the art would not turn to the document of Alkhatib since the document of Alkhatib refers to a virtual community network (VCN) in which a user being a member of a community needs to join the network to become a member of the VCN as described in paragraph [0146]. A person of ordinary skill in the art would simply have no reason to combine Briscoe and Alkhatib.

Nevertheless, for the sake of including an argument regarding this point on the record, if a person skilled in the art combined the teaching of Briscoe with the teaching of Alkhatib, such combination would not lead to the solution offered by the present invention as defined by the present claims since Alkhatib discloses a virtual community network (VCN) having a VCN manager controlling a server which a member can join via a series of procedures which do not simplify the method disclosed by Briscoe. The method disclosed by Alkhatib comprises a first step for member registration, as described in paragraph [0126], and a second step for a member to join or leave, as described in paragraph [0145]. The step for member registration is comparable to the step of distribution of authentication information disclosed by Briscoe and is subdivided into a registration request and a registration file request, as described in paragraph [0127]. During the step for member registration, a non-registered member of a community receives, after exchange of a plurality of data packets with the VCN manager, an acknowledgement packet comprising a crypto-type indicating how the rest of the packet is encrypted and a registration file comprising a number of fields containing the information required by the member to successfully perform a join, as described in paragraphs [0138]-[0140]. One of the fields of the registration file is a token key which is the shared secret between the VCN manager and the member, as described in paragraph [0141]. Once a user is registered, the user can join the VCN through a join operation comprising an initialize request and an actual join, as described in paragraph [0147]. The second step of member join/leave corresponds to an authentication procedure, as described in paragraphs [0146]-[0148], in which a member agent initially sends an init request packet to the VCN manager, the packet comprising a plurality of information items such as a member seed (a random number), as described in paragraphs [0149]-[0151]. If the member passes authentication, the VCN manager sends an acknowledgement packet to the member, which packet contains a plurality of parameters which are different than the information items of the

init request packet. It is noted that the parameters used in the authentication procedure disclosed by Alkhatib, as well as the parameters used in the authentication procedure disclosed by Briscoe, are different than the parameters used in the present invention as recited in the claims.

Further, it is noted that Alkhatib does not disclose the criteria used by the VCN manager to acknowledge authentication (see, e.g., paragraphs [0154]-[0155]). In contrast to the present invention as recited in the claims, Alkhatib does not disclose an authentication procedure utilizing a challenge response pattern, at least not the challenge response pattern disclosed in independent claim 1, which is based on the computation of a hash value at the server side and a hash value at the client side and the comparison of these two hash values by the server. It is further noted that Briscoe also does not disclose the comparison of two hash values during its authentication procedure.

Combining the teachings of Briscoe and Alkhatib, a person skilled in the art would instead be led to a two-step procedure where the first step involves distribution of authentication information among the clients within the network, whereas the second step involves the authentication. In the first step, the exchanged information would be transformed into hash values; however, there would be several transmissions of the information between the server and the client.

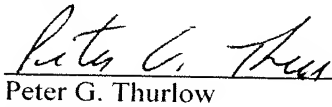
Further, Alkhatib neither suggests nor teaches the use of a hash algorithm for a data packet during authentication but, instead, teaches such during a registration step. Referring to the registration step, a registration authenticator is computed using the first sixteen bytes of a HMAC-SHA-1 applied to a packet data, as described in paragraph [0133], which packet data comprises the client fully qualified domain name (FQDN), a Diffe-Hellman key exchange request to the VCN manager, a packet version information, type and length information, a user authenticator, the length of FQDN in octets, a VCN name offset, the member's FQDN in DNS format, the length of Diffe-Hellman value in octets and the member's initial Diffe-Hellman value, as described in paragraph [0131]. It is noted that the parameters used to compute the hash value of the present invention as recited in the claims, i.e. the parameters client password, the client computer's unique IP address, the server unique IP address and a nonce value, are different than such parameters. It is also noted that the references cited in the office action relate to a first step of distribution of authentication information based on Briscoe and to a second step of authentication based on Alkhatib. It would therefore not be

obvious for a person skilled in the art to combine these different features and achieve one single authentication procedure such as that of the present invention as defined by the claims.

In light of the above remarks, the Applicant respectfully requests that the Examiner reconsider this application with a view towards allowance. The Examiner is invited to call the undersigned attorney if a telephone call could help resolve any remaining items.

Respectfully submitted,

Date: November 29, 2007



47,138
Peter G. Thurlow (Reg. No.)

JONES DAY
222 East 41st Street
New York, New York 10017-6702
(212) 326-3694